

CDC & ATSDR SECURITY STANDARDS
for
NOVELL FILE SERVERS

These security standards represent minimal acceptable file server security safeguards at CDC and their implementation is not optional.

PASSWORDS

1. Require all accounts to have a password. The password must be least 6 characters long.
2. Force periodic change of password at least every 90 days.
3. Require unique passwords (prevents users from switching between 2 or 3 passwords). The Novell software defaults to remember the last 8 passwords that have been used. The value of 8 is currently fixed and cannot be easily altered.
4. Prohibit "password piping" from any source (e.g., BAT files, script files, keyboard stuffers) which is not "station restricted."

SUPERVISOR ACCOUNTS

1. Each file server shall have an LAN administrator and at least one alternate, but not more than two alternate administrators with access to the SUPERVISOR account and console passwords.
2. A backup account with supervisory equivalence is required for nightly system tape backups; only the LAN Administrator and alternate(s) should have this password. This account will be limited to ONE concurrent login and will be restricted to ONE workstation address. The name of the backup account should be unique and not generally known. Obviously, it should not be called BACKUP.
3. The file server console/monitor will be locked using the Novell keyboard lock utility. Only the LAN Administrator and alternate(s) will have this password. All file server and/or router equipment will be located in areas that are physically secured during non-business hours. Minimum physical security safeguards shall consist of floor to ceiling walls, and door/window locks. These areas must provide controlled access at all times.

4. The Rconsole, console keyboard, backup, and SUPERVISOR passwords will be changed at least every 90 days.

LOGIN RESTRICTIONS

1. Limit all accounts (including SUPERVISOR and "backup") to ONE concurrent connection to the file server except for LAN Administrators who can have TWO and programmers who can have up as many as necessary to do their job.

2. Limit access to authorized agency employees, contractors, or others engaged in official agency business. All contractors, nonpermanent employees, and other temporary accounts should be set with SPECIFIC and REALISTIC expiration date limits.

3. Never create an account using common or easily predictable names (passworded or not). Examples of names to AVOID are: GUEST, VISITOR, BACKUP, DEMO

4. Inactive user accounts should be identified and deleted immediately. Inactive accounts are those special cases where the expiration date has passed (see item 2 above). If an employee moves from LAN to LAN, files may be moved with them.

5. A user account should be automatically locked out after five incorrect password attempts. Restoration of service will require intervention of an account administrator.

FILE SERVER BACKUP PROCEDURES

1. Backup data nightly.

2. Store backup tapes in an area away from the IRM equipment area. Keep tapes for at least 35 calendar days or 24 backup days, whichever is greater. Rotate tape sets periodically.

3. Since backup tape verification during backup is not always reliable, backup sets should be verified at least twice a month by attempting to restore one or more files from the backup.

4. While not required, use of off-site storage should be considered for back up tapes. IRMO maintains a contract with a commercial off-site storage facility which can be used for this purpose.

VIRUS SCANNING

1. Use Novell file access rights to protect all infectable files (e.g., COM, EXE, etc.). Security, such as the read only flag is NOT sufficient since it can be attacked by a virus.
2. If a virus infection is detected on a file server or on workstations within a network, the network involved must be removed immediately from the CDC backbone, if appropriate to protect other WAN resources. The involved LAN Administrator, IRM Coordinator, and appropriate IRMO staff should be notified as soon as possible.
3. All Level I (CDC & ATSDR Microcomputer and LAN Standards/Guidelines) anti-virus scan software must reside on every file server. This same Level I anti-virus scan software must be readily available to end-users who need to scan their individual workstations. All file servers should be constantly monitored by a resident Level I NLM virus detection system which uses virus signatures and check summing.

LAN WORKSTATION STANDARDS (as they relate to file server security)

1. All workstations running Microsoft Windows 95 (or higher) will activate the password option of the desktop screen saver. This will invoke a keyboard lock if the user does not enter a keystroke for a period not to exceed 15 minutes.
2. All keyboard locking software will be set to require the user to enter a password at least 6 characters in length
3. Workstations will be scanned daily for viruses. Scanning should not be user optional. LAN Administrators are encouraged to automate this process.